CURRENT CHALLENGES IN COMPUTER SECURITY PROGRAM MANAGEMENT

Panelists:

Barbara Guttman
National Institute of Standards and Technology
Building 820, Room 426
Gaithersburg, MD 20899
e-mail: barbara.guttman@nist.gov

Lynn McNulty
McNulty and Associates
P.O. Box 6101
McLean, VA 22106
e-mail: LYNN.McNULTY@INTERNETMCI.COM

Paul M. Connelly
Chief, Security and Safety Division
White House Communications Agency
The White House
Washington, D.C. 20500

Ann F. Miller
Fleet and Industrial Supply Center
Code 12/80.1
1968 Gilbert Street
Norfolk, VA 23511-3318
e-mail: ANN_MILLER@WP-EMH1.NOR.FISC.NAVY.MIL

Mark Wilson (Panel Chair)
National Institute of Standards and Technology
Building 820, Room 426
Gaithersburg, MD 20899
e-mail: mark.wilson@nist.gov

PANEL SUMMARY

Managing a computer security program has been getting more difficult in light of budget constraints, reorganizing and downsizing, and the continuing decentralization of ever-increasingly complex computing and communications environments. This panel will discuss the changes in OMB Circular A-130 and the document's impact on computer security programs, the marketing of a computer security program, how to build a successful program, how to keep a program stable during unstable times - during a reorganization, and the efffective use of collateral-duty personnel to support and augment the computer security staff.

Barbara Guttman, NIST - A new version of OMB Circular A-130 was signed on February 8, 1996. The Circular provides uniform government-wide information resources management policies, including computer security policies. The main thrust of the new version of the Circular is to drive security responsibilities down to the users and managers of computer systems and information. To address computer security in today's environments, users and managers need a framework which can handle a myriad of technological possibilities. The Circular suggests a structure with two categories: general support systems and major applications. Another important change in the structure is that the new A-130 does not distinguish between "sensitive" and "non-sensitive" systems. These and other changes will be discussed.

Lynn McNulty, McNulty and Associates - Knowing the computer security requirements is only the beginning. A newly-appointed computer security officer, or a veteran in a newly-established computer security program must to be able to convince often-sceptical agency executives, managers, and users that computer security is important, why it is important, and why computer security needs to be integrated into the agency's business and decision-making process. Useful strategies for working with these audiences, getting others to accept the responsibility for "doing" computer security, as well as how to better your chances of winning budget and people battles will be discussed.

Paul M. Connelly, White House Communications Agency - This presentation contains first-hand examples of how a successful computer security program was built using these strategies. Topics that will be discussed include how a security program was built from scratch to protect some of our nation's most sensitive and critical information systems in a highly operations-driven environment, and obtaining management buy-in (e.g., identifying key allies, involving management in setting program goals and priorities, and obtaining management committment for specific objectives). The speaker will also address what worked, what did not work, obstacles faced, and will offer a recipe for success.

Ann F. Miller, Fleet & Industrial Supply Center, Norfolk (Department of the Navy) - Once a computer security program matures, it still faces a number of pitfalls. One challenge that program managers face today is keeping a successful security program intact during a reorganization, or a series of reorganizations. Topics including policy and procedure enforcement, changing management structures and reporting paths, establishing security agreements between new or changing organizations, inspections and compliance checks, preparing for inspector general (IG) visits, and keeping up with the changes to the network of collateral-duty security personnel will be discussed.

Mark Wilson, National Institute of Standards and Technology - One tool in the computer security officer's toolkit to meet today's funding challenge is the effective use of collateral-duty security personnel. Some agencies have found that a network of collateral-duty personnel, appointed for each network and system in an agency, makes implementation and maintenance of policy, procedures, and practices more manageable, negates the possible impact of distances between some agency offices, and provides easier individual identification and auditability for the computer security officer. Utilization of this approach can help spread the workload more evenly among system users and system administrators. This can also increase the agency-wide awareness of information systems security responsibilities, while utilizing the existing management structure.